CLAIMS

What is claimed is:

1. A method for symmetric-key encrypted transmission of block-organized data between a sender and receiver comprising the following steps, in order:

(a) exchanging a initialization string by secure, external means between sender and receiver;

(b) generating an encryption key by pseudo-random-function means operating on data comprising the initialization string at both sender and receiver;

(c) encrypting the next block of data into ciphertext by symmetric-key-encryption algorithm means comprising the encryption key at the sender;

(d) transmitting the ciphertext to the receiver;

(e) decrypting the ciphertext by symmetric-key-encryption algorithm means comprising the encryption key at the receiver;

(f) generating a new encryption key at both sender and receiver by pseudo-random-function means operating on data comprising the previous encryption key; and

repeating the steps from (d) forward repeatedly until the data is exhausted.

2. The method of claim 1, further comprising:

calculating synchronization data at sender and receiver by pseudo-random function means operating on data comprising the current data block;

including the synchronization data with the ciphertext transmitted to the receiver;

comparing the synchronization data received with the synchronization calculated;

signaling resynchronization requests from receiver to sender;

acknowledging resynchronization requests; and

re-executing the steps of claim 1. From step (d) forward.

3. The method of claim 2, further comprising adding entropy to new encryption key by pseudo-random-function means operating on the data block.

4. The method of claim 2, wherein the pseudo-random-function means operating on the data block further comprises function means operating on the ciphertext.

5. A method for symmetric-key encrypted transmission of data between a sender and receiver comprising the following steps, in order:

(a) exchanging a initialization string by secure, external transmission between sender and receiver;

(b) generating an encryption key by pseudo-random-function means operating on data comprising the initialization string at both sender and receiver;

(c) encrypting the next block of data into ciphertext by symmetric-key-encryption algorithm means comprising the encryption key at the sender;

(d) transmitting the ciphertext to the receiver;

(e) decrypting the ciphertext by symmetric-key-encryption algorithm means comprising the encryption key at the receiver;

(f) generating a new encryption key at both sender and receiver by pseudo-random-function means operating on data comprising the initialization string; and

repeating the steps from (d) forward repeatedly until the data is

exhausted.

6. The method of claim 5, further comprising:

calculating synchronization data at sender and receiver by pseudo-random function means operating on data comprising the current data block;

including the synchronization data with the ciphertext transmitted to the receiver;

comparing the synchronization data received with the synchronization calculated;

signaling resynchronization requests from receiver to sender;

acknowledging resynchronization requests; and

re-executing the steps of claim 5 from step (d) forward.

7. The method of claim 6, further comprising adding entropy to new encryption key by pseudo-random-function means operating on the data block.

8. The method of claim 6, wherein the pseudo-random-function means operating on the data block further comprises function means operating on the ciphertext.

9. A method for symmetric-key encrypted transmission of block-organized data between a sender and receiver comprising the following steps, in order:

(a) exchanging a initialization string by secure, external means between sender and receiver;

(b) generating one or more intermediate keys by pseudo-random-function means operating on data comprising the initialization string at both sender and receiver;

(c) generating an encryption key by pseudo-random-function means operating on data comprising the intermediate keys at both sender

and receiver;

(d) encrypting the next block of data into ciphertext by symmetric-key-encryption algorithm means comprising the encryption key at the sender;

(e) transmitting the ciphertext to the receiver;

(f) decrypting the ciphertext by symmetric-key-encryption algorithm means comprising the encryption key at the receiver;

(g) generating new intermediate keys at both sender and receiver by pseudo-random-function means operating on data comprising the previous intermediate keys; and

repeating the steps from (c) forward repeatedly until the data is exhausted.

10. The method of claim 9, further comprising:

calculating synchronization data at sender and receiver by pseudo-random function means operating on data comprising the current data block;

including the synchronization data with the ciphertext transmitted to the receiver;

comparing the synchronization data received with the synchronization calculated;

signaling resynchronization requests from receiver to sender;

acknowledging resynchronization requests; and

re-executing the steps of claim 9 from step (c) forward.

11. The method of claim 10, further comprising adding entropy to new encryption key by pseudo-random-function means operating on the data block.

12. The method of claim 11, wherein the pseudo-random-function means operating on the data block further comprises function means operating on the ciphertext.

13. A method for symmetric-key encrypted transmission of data between a sender and receiver comprising the following steps, in order:

(a) exchanging a initialization string by secure, external transmission between sender and receiver;

(b) generating a master recovery key by pseudo-random function means from data comprising the initialization string;

(c) generating a first intermediate key by pseudo-random-function means operating on data comprising the master recovery key at both sender and receiver;

(d) generating one or more second keys by pseudo-random-function means operating on data comprising the first intermediate key at both sender and receiver;

(e) generating an encryption key by pseudo-random-function means operating on data comprising the second intermediate keys at both sender and receiver;

(f) encrypting the next block of data into ciphertext by symmetric-key-encryption algorithm means comprising the encryption key at the sender;

(g) transmitting the ciphertext to the receiver;

(h) decrypting the ciphertext by symmetric-key-encryption algorithm means comprising the encryption key at the receiver;

(i) generating new second intermediate keys at both sender and receiver by pseudo-random-function means operating on data comprising the previous intermediate keys; and

repeating the steps from (d) forward repeatedly until the data is exhausted.

14. The method of claim 13, wherein synchronization correcting further comprises:

calculating synchronization data at sender and receiver by pseudo-random-function means operating on data comprising the current data block;

including the synchronization data with the ciphertext transmitted to the receiver;

comparing the synchronization data received with the synchronization calculated;

signaling resynchronization requests from receiver to sender;

acknowledging resynchronization requests; and

re-executing the steps of claim 13 from step (c) forward.

15. The method of claim 14, further comprising adding entropy to new encryption key by pseudo-random-function means operating on the data block.

16. The method of claim 14, wherein the pseudo-random-function means operating on the data block further comprises function means operating on the ciphertext.

17. The method of claim 14, wherein the first intermediate key comprises the Master Key, and wherein the second intermediate keys comprise the Internal key.

18. A method for generating and updating encryption keys for use in symmetric-key encrypted transmission between a sender and receiver, in which pre-existing host software includes encryption and decryption algorithms and further includes signaling means, comprising the following steps, in order:

(a) exchanging a initialization string by secure, external means between sender and receiver;

(b) generating an encryption key by pseudo-random-function means operating on data comprising the initialization string at both

sender and receiver;

(c) repeating the steps from (b) forward when signaled by the host software.

19. The method of claim 18, in which the host software organizes the data in one or more data blocks, and in which the data is enciphered by the host software into ciphertext, further comprising adding entropy to new encryption key by pseudo-random-function means operating on the data block.

20. The method of claim 19, further comprising:

a) calculating synchronization data at sender and receiver by pseudo-random function means operating on data comprising the current data block;

b) including the synchronization data with the ciphertext transmitted to the receiver;

c) comparing the synchronization data received with the synchronization calculated;

d) signaling re-synchronization requests and acknowledgments between receiver and sender;

e) re-executing the steps of claim 18 from step (b) forward.

21. A method for generating and updating encryption keys for use in symmetric-key encrypted transmission between a sender and receiver, in which pre-existing host software includes encryption and decryption algorithms and further includes signaling means, comprising the following steps, in order:

a) exchanging an initialization string by secure, external means between sender and receiver;

b) generating one or more intermediate keys by pseudo-random-function means operating on data comprising the initialization string at

both sender and receiver;

c) generating an encryption key by pseudo-random-function means operating on data comprising the intermediate keys at both sender and receiver;

d) generating new intermediate keys at both sender and receiver by pseudo-random-function means operating on data comprising the previous intermediate keys; and

e) repeating the steps from (b) forward repeatedly when signaled by the host software.

22. The method of claim 21, in which the host software organizes the data in one or more data blocks, and in which the data is enciphered by the host software into ciphertext, further comprising adding entropy to new encryption key by pseudo-random-function means operating on the data block.

23. The method of claim 22, further comprising:

a) calculating synchronization data at sender and receiver by pseudo-random function means operating on data comprising the current data block;

b) including the synchronization data with the ciphertext transmitted to the receiver;

c) comparing the synchronization data received with the synchronization calculated;

d) signaling re-synchronization requests and acknowledgments between receiver and sender; and

re-executing the steps of claim 18 from step (b) forward.

24. The method of claim 1, further including an authentication method which comprises

generating an authentication code by function means operating on data comprising the initialization string at both sender and receiver;

transmitting the authentication code from sender to receiver, said code constituting a remote code at the receiver;

transmitting the authentication code from receiver to sender , said code constituting a remote code at the sender;

comparing the remote code to the generated code at both sender and receiver;

transmitting an authentication error from receiver to sender when the receiver remote code does not correspond to the receiver generated code; and

transmitting an authentication error from sender to receiver when the sender remote code does not correspond to the sender generated code.

25. The method of claim 9, further including an authentication method which comprises:

generating an authentication code by function means operating on data comprising one or more intermediate keys at both sender and receiver;

transmitting the authentication code from sender to receiver, said code constituting a remote code at the receiver;

transmitting the authentication code from receiver to sender , said code constituting a remote code at the sender;

comparing the remote code to the generated code at both sender and receiver;

transmitting an authentication error from receiver to sender when the receiver remote code does not correspond to the receiver generated

code; and

transmitting an authentication error from sender to receiver when the sender remote code does not correspond to the sender generated code.

26. The method of claim 17, further including an authentication method which comprises:

generating an authentication code by function means operating on data comprising the Master Key at both sender and receiver;

transmitting the authentication code from sender to receiver, said code constituting a remote code at the receiver;

transmitting the authentication code from receiver to sender , said code constituting a remote code at the sender;

comparing the remote code to the generated code at both sender and receiver;

transmitting an authentication error from receiver to sender when the receiver remote code does not correspond to the receiver generated code; and

transmitting an authentication error from sender to receiver when the sender remote code does not correspond to the sender generated code.